UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,745	05/09/2001	William Rex Akers	HTHC 3423000	3915

21909 7590 05/22/2007

CARR LLP
670 FOUNDERS SQUARE
900 JACKSON STREET
DALLAS, TX 75202

EXAMINER	
MORGAN, ROBERT W	
ART UNIT	PAPER NUMBER
3626	

MAIL DATE	DELIVERY MODE
05/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/851,745	AKERS ET AL.	
	Examiner	Art Unit	
	Robert W. Morgan	3626	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/9/07 has been entered.

Notice to Applicant

2. This communication is in response to the amendment filed 3/11/03. Claims 1, 10, 23, 24 and 27 have been amended. Claims 1-35 are presented for examination.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1 and 10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear how encapsulation data is used to determine whether the medical record data file has been altered by the record client or modified at the remote location. For examination purposes the Examiner has treated encapsulated data as used to add security and privacy to data.

NOTE: Claims 2-9 and 11-19 incorporate the deficiencies of claims 1 and 10 are therefore rejected for the same reasons as those claims.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,924,074 to Evans in view of U.S. Patent No. 7,039,810 to Nichols.

As per claim 1, Evans teaches a system for transferring electronic medical files comprising:

--the claimed record client coupled to the record server, the record client receiving the medical record data file is met by the electronic medical record system that includes a server (406, Fig. 24) connected to client machines running application such as Microsoft Windows to access the data (see: column 14, lines 8-16); and

Evans teaches an electronic medical record system that includes remote web servers (406, 408, 410, Fig. 24) with medical record information (see: column 12, lines 56-63)

Evans fails to teach:

--the claimed record encapsulation system generating encapsulation data of a medical record data file;

--the claimed record server encrypting the encapsulated medical record data file and transmitting the encrypted, encapsulated medical record data file; and

--the claimed encapsulation data is used to determine whether the medical record data file has been altered by the record client.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15). Data encryption has been increasingly used to add security and privacy to data, voice and video transmissions across public networks (see: column 2, lines 54-56).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include encryption of medical information as taught by Nichols within the electronic medical record system as taught by Evans with the motivation of providing an apparatus and method for securely transferring sensitive information, such as patient information using encryption methods to prevent abuse (see: Nichols: column 1, lines 19-24).

As per claim 2, Evans teaches the claimed record server further comprises a sync system verifying that the record client has received a sync file before transferring the medical record data file. This feature is met by the electronic medical record system including web servers (406, Fig. 24) that allow patient data to be transfer between external source as well as updating the patient record obviously suggesting that the comparing and checking of medical data take place to verify that an up-to-date medical record is available (see: column 3, lines 37-43 and column 5, lines 36-40).

As per claim 3, Evans teaches the claimed record server further comprises a tracking system updating a tracking record when the medical record data file is transferred. This feature is met by the tracking and description of patient data within the system (see: column 9, lines 27-37).

As per claim 4, Evans teaches the claimed record client further comprises a tracking system updating a tracking record when the medical record data file is accessed. This limitation is met by the electronic medical record system which updates patient's records upon a nurses or physician entry of information into the system (see: column 5, lines 29-40).

As per claim 5, Evans teaches the claimed record client further comprises a remote data system, the remote data system generating medical record data. This limitation is met by the electronic medical record system that includes server (406 Fig. 24) that are connected to client machines running application such as Microsoft Windows to access and generating medical data (see: column 14, lines 8-16).

Evans fails to teach the claimed record client encapsulates the medical record data to prevent it from being modified.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15). Data encryption has been increasingly used to add security and privacy to data, voice and video transmissions across public networks (see: column 2, lines 54-56).

The obviousness of combining the teachings of Nichols with the system as taught by Evans are discussed in the rejection of claim 1, and incorporated herein.

As per claim 6, limitations with respect to the claimed record client system further comprises a detail encapsulation system receiving comment data and encapsulating the comment data to prevent it from being modified are met by Nichols teaching of sensitive data such as

patient records securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15).

The obviousness of combining the teachings of Nichols with the system as taught by Evans are discussed in the rejection of claim 1, and incorporated herein.

As per claim 7, the feature of the claimed record server further comprises a record storage system, the record storage system storing each version of the medical record data file received by the record server is met by the teaching of Evans of organizing and storing of patient medical records in which are made available for access by authorized personnel (see: column 2, lines 65 to column 3, lines 3).

As per claim 8, Evans teaches the claimed record server further comprises an excerpt transfer system, the excerpt transfer system receiving medical record excerpt data and transferring it to a predetermined recipient. This feature is met by the transferred patient data from the electronic medical records system to other healthcare providers (see: column 4, lines 64 to column 5, lines 8).

As per claim 9, Evans teaches the claimed notification system transferring notification data to a party regarding the availability of medical record data. This data is met by the acknowledgment by the healthcare provider that a patient's record has been reviewed and adding to the medical record any necessary instructions or recommendations for treatment (see: column 2, lines 45-58).

As per claim 10, Evans teaches the claimed a method for transferring electronic medical files comprising:

--the claimed assembling the medical record data into a medical record data file is met by the storing and organizing of patient records in a patient repository (see: column 3, lines 9-16);

--the claimed receiving a request to transfer the medical record data file is met by the point of care system issuing a request to transfer patient data (see: column 9, lines 39-53); and

--the claimed transferring the medical record data file to a remote location is met by the transferring of patient data between external sources (see: column 3, lines 36-42).

Evans fails to teach:

--the claimed generating encapsulating of medical record data.

--the claimed encrypting the medical record data for data transmission security;

--the claimed decrypting the medical record data file at the remote location after it has been received; and

--the claimed using the encapsulation data to determine whether the medical record data has been modified at the remote location.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15). Additionally, Nichols teaches that a remote data center (224, Fig. 5) receives encrypted sensitive information (221, Fig. 5) transmitted by programmer (222, Fig. 5) and the decryption engine (234, Fig. 5) that resides on the remote data center (224, Fig. 5) decrypts the encrypted sensitive

information (221, Fig. 5). Data encryption has been increasingly used to add security and privacy to data, voice and video transmissions across public networks (see: column 2, lines 54-56).

The obviousness of combining the teachings of Nichols with the system as taught by Evans are discussed in the rejection of claim 1, and incorporated herein.

As per claim 11, Evans teaches the claimed transferring the medical record data file to the remote location further comprises transferring a sync file to the remote location. This limitation is met by the transferring of patient data between external sources (see: column 3, lines 36-42).

As per claim 12, Evans teaches the claimed assembling the medical record data into the medical record data file further comprises storing a tracking record with the medical record data file. This feature is met by the electronic medical record system which stores and updates patient records upon a nurses or physician entry of information (see: column 3, lines 9-16 and column 5, lines 29-40).

As per claim 13, Evans teaches the claimed generating notification data at the remote location. This limitation is met by the acknowledgment by the healthcare provider that a patient's record has been reviewed and adding to the medical record any necessary instructions or recommendations for treatment (see: column 2, lines 45-58).

As per claim 14, Evans teaches the claimed accessing the medical record data file at the remote location (see: column 2, lines 45-47); and

--the claimed updating a tracking record to show that the medical record data file has been accessed at the remote location is met by the electronic medical record system which allows nurses and physician to access and update patient's records upon entry into the system (see: column 5, lines 29-40).

As per claim 15, Evans teaches the claimed receiving medical record data at the remote location (see: column 10, lines 18-23); and

--the claimed updating the medical record data file to include the medical record data is met by the electronic medical record system which allows nurses and physician to access and update patient's records upon entry into the system (see: column 5, lines 29-40).

Evans fails to teach the claimed encapsulating the medical record data to prevent the medical record data from being modified.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15). Additionally, Nichols teaches that a remote data center (224, Fig. 5) receives encrypted sensitive information (221, Fig. 5) transmitted by programmer (222, Fig. 5) and the decryption engine (234, Fig. 5) that resides on the remote data center (224, Fig. 5) decrypts the encrypted sensitive information (221, Fig. 5). Data encryption has been increasingly used to add security and privacy to data, voice and video transmissions across public networks (see: column 2, lines 54-56).

The obviousness of combining the teachings of Nichols with the system as taught by Evans are discussed in the rejection of claim 1, and incorporated herein.

6. Claims 16-17, 19 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,924,074 to Evans in view of U.S. Patent No. 6,305,377 to Portwood et al.

As per claim 16, Evans teaches the claimed record server and record client coupled to the record server (see: column 14, lines 8-16).

Evans fails to teach the claimed distributing of medical supplies and receiving package data from the record server with verification data and correlating the verification data to the package data.

Portwood et al. teach a prescription distribution system including a server computer communicating with other prescriber computer to transfer prescription data to the server for validation, certification, and distribution (see: abstract, column 3, lines 43-49 and column 7, lines 35-37). It is respectfully submitted that prescriptions are a form of "medical supplies".

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention to include the prescription distribution system as taught by Portwood et al. with the electronic medical record system as taught by Evans with the motivation of streamlining and incorporating automatic mail ordering, billing, and other business aspects, such as prescription verification and delivery (see: Portwood et al. column 2, lines 9-13).

As per claim 17, Evans teaches the claimed tracking system that includes tracking and description of patient data within the system (see: column 9, lines 27-37).

Evans fails to teach the receiving of verification and incrementing order data.

Portwood et al. teaches the claimed transferring of prescription data to the server for validation, certification, and distribution as well a ordering system for prescription refills for the patient (see: column 2, lines 44-46 and column 7, lines 35-37).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention to include the prescription distribution system as taught by Portwood et al. with the electronic medical record system as taught by Evans with the motivation of streamlining and

incorporating automatic mail ordering, billing, and other business aspects, such as prescription verification and delivery (see: Portwood et al. column 2, lines 9-13).

As per claim 19, Evans teaches the claimed record client further comprises a remote data system, the remote data system generating counseling data and transmitting the counseling data to the record server. This limitation is met by access of the patient record from any geographical location as well as providing prescription instruction to a patients record (see: column 2, lines 45-58).

As per claim 35, Evans teaches the record client further comprises an image data capture device that generates image data, and the verification data includes the image data. This features is met by the data source (370, Fig. 23) that comprises physical data (374, Fig. 23) such as paper based records and photographs, and electronic mainframe data (376, Fig. 24). The converter (372, Fig. 24) receives information from the data source (370, Fig. 24) and transforms the information into an electronic format compatible with the EMR system. For example, to input physical data (374, Fig. 24) such as paper or image based data, into a patient record, the converter (372, Fig. 24) comprises a scanner to digitize the physical data into a binary file format for incorporation into the patient's record (see: column 12, lines 35-46).

7. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,924,074 and U.S. Patent No. 6,305,377 to Portwood et al. as applied to claim 16 above, and further in view of U.S. Patent No. 7,039,810 to Nichols.

As per claim 18, Evans in combination with Portwood et al. teaches a system with a record server that verifies the data in a medical record data file. However, Evans in combination with Portwood et al. fails to teach the encapsulating of the verification data.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15). Additionally, Nichols teaches that a remote data center (224, Fig. 5) receives encrypted sensitive information (221, Fig. 5) transmitted by programmer (222, Fig. 5) and decrypts the encrypted sensitive information (221, Fig. 5). Data encryption has been increasingly used to add security and privacy to data, voice and video transmission across public networks (see: column 2, lines 54-56).

One of ordinary skill in the art at the time the invention was made would have found it obvious to include encryption of medical information as taught by Nichols within the combination of the electronic medical record system as taught by Evans and the prescription distribution system as taught by Portwood et al. with the motivation of providing an apparatus and method for securely transferring sensitive information such as patient information using encryption methods to prevent abuse (see: Nichols: column 1, lines 19-24).

8. Claims 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,305,377 to Portwood et al. in view of U.S. Patent No. 5,924,074 to Evans.

As per claim 20, Portwood et al. teaches a method for distributing medical supplies comprising:

--the claimed storing package data corresponding to a sealed package is met by the data storage unit use to store patient data including prescription data (see: column 2, lines 60-66);

--the claimed transmitting the sealed package to a remote site is met by the prescription distribution system that enable quicker delivery of prescription at the patient's location (see: abstract and column 5, lines 7-10); and

--the claimed authorizing release of the package if the stored package data matches the received package data is met by the prescription delivery message system that includes a message receiving unit connected to the CPU to receive the prescription delivery message upon delivery of the prescription and the matching of prescription data (see: column 3, lines 36-41).

Portwood et al. fails to teach the claimed receiving the package data from the remote site.

Evans teaches a system for instant access to a patient's electronic medical record from any geographical location and the transferring and receiving patient record external sources (see: column 2, lines 45-47 and column 10, lines 18-23).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention to include the electronic medical record system as taught by Evans with the prescription distribution system as taught by Portwood et al. with the motivation of streamlining and incorporating automatic mail ordering, billing, and other business aspects, such as prescription verification and delivery (see: Portwood et al. column 2, lines 9-13).

As per claim 21, Portwood et al. teaches the claimed receiving the package data from the remote site further comprises: counseling a patient if the patient has not received the medical supplies before; and generating counseling data is met by the prescription message that includes instruction on how to take the medication or how to conduct various medical procedures (see: column 17, lines 17-22).

As per claim 22, Portwood et al. teaches the claimed incrementing order data after the package is released is met by the ordering of prescription refills which enable the system to keep track to increase or decrease a refill of a patient prescription (see: column 2, lines 44-47).

9. Claims 23, 28-29, 30-31 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,924,074 to Evans in view of U.S. Patent No. 7,039,810 to Nichols.

As per claim 23, Evans teaches an electronic medical record system that includes remote servers (406, 408, 410, Fig. 24) with medical record information (see: column 12, lines 56-63). The remote servers are connected to client machines running applications such as Microsoft Windows to access (see: column 14, lines 8-16). In addition, the web servers (406, Fig. 24) allows patient data to be transfer between external source as well as updating the patient record upon a nurse or physician entry of information into the system (see: column 5, lines 29-40 and column 9, lines 27-37). This suggests that comparing and checking of medical takes place to verify that an up-to-date medical record is available and is transferred to an external source updated or not (see: column 3, lines 37-43 and column 5, lines 36-40). Evans further teaches a tiered password system to ensure patient confidentiality and provides several levels of security for access to patient data this suggests a nurse with the authorization to view the entire patient record may only update certain aspects according to the level of authorization (see: column 15, lines 9-32).

Evans fails to teach detail encapsulation system for receiving data and preventing it from being modified.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15). Additionally, Nichols teaches that a remote data center (224, Fig. 5) receives encrypted sensitive information (221, Fig. 5) transmitted by programmer (222, Fig. 5) and the decryption engine (234, Fig. 5) that resides on the remote data center (224, Fig. 5) decrypts the encrypted sensitive information (221, Fig. 5). Data encryption has been increasingly used to add security and privacy to data, voice and video transmissions across public networks (see: column 2, lines 54-56).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include encryption of medical information which is a form of encapsulation as taught by Nichols within the electronic medical record system as taught by Evans with the motivation of providing an apparatus and method for securely transferring sensitive information, such as patient information using encryption methods to prevent abuse (see: Nichols: column 1, lines 19-24).

As per claim 28, Evans teaches an electronic medical record system that transfers patient data from the electronic medical records system to other healthcare providers and between external sources (see: column 3, lines 36-42 and column 4, lines 64 to column 5, lines 8).

Evans fails to explicitly teach extracting an excerpt of the electronic medical record data from the electronic medical record data file comprises removing user readable patient identifying data.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by an encryption engine (230, Fig. 5). The Examiner considers the encrypting of the patient records to include removing user readable patient identifying data to protect confidentiality of patient's medical information.

The obviousness of combining the teaching of Nichols and Evans are discussed in the rejection of claim 23, and incorporated herein.

As per claim 29, Evans teaches an electronic medical record system that includes remote servers (406, 408, 410, Fig. 24) with medical record information (see: column 12, lines 56-63). The remote servers are connected to client machines running applications such as Microsoft Windows to access (see: column 14, lines 8-16). In addition, the web servers (406, Fig. 24) allows patient data to be transfer between external source as well as updating the patient record upon a nurse or physician entry of information into the system (see: column 5, lines 29-40 and column 9, lines 27-37). This suggests that comparing and checking of medical is taking place to verify that an up-to-date medical record is available (see: column 3, lines 37-43 and column 5, lines 36-40). Evans further teaches a tiered password system to ensure patient confidentiality and provides several levels of security for access to patient data this suggests a nurse with the authorization to view the entire patient record may only update certain aspects according to the level of authorization (see: column 15, lines 9-32).

Evans fails to teach the encapsulating an electronic medical record file to prevent it from being modified and decrypting the encrypted encapsulated electronic medical record file at the remote location.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15). Additionally, Nichols teaches that a remote data center (224, Fig. 5) receives encrypted sensitive information (221, Fig. 5) transmitted by programmer (222, Fig. 5) and the decryption engine (234, Fig. 5) that resides on the remote data center (224, Fig. 5) decrypts the encrypted sensitive information (221, Fig. 5). Data encryption has been increasingly used to add security and privacy to data, voice and video transmissions across public networks (see: column 2, lines 54-56). The Examiner considers decrypting the medical file at a remote location to include in order for the information to be added to view by an authorized user.

The obviousness of combining the teaching of Nichols and Evans are discussed in the rejection of claim 23, and incorporated herein.

As per claim 30, Evans teaches an electronic medical record file is an image data file. This limitation is met by the patient data structure (210, Fig. 13) that maintain a pointer to a legacy files structure (219, Fig. 13) having patient data transmitted from the legacy data system (106, Fig. 1), such as an image of a patient chart (see: column 8, lines 57-60).

As per claim 31, Evans teaches the sync file is a patient file. This feature is met by the electronic medical record system including web servers (406, Fig. 24) that allow patient data to

be transfer between external sources as well as updating the patient record (see: column 3, lines 37-43 and column 5, lines 36-40). The Examiner considers the updated patient record to be the sync file, which is already compared and checked to verify the availability of an up-to-date medical record.

As per claim 33, Evans teaches transferring the sync file comprises creating a patient folder. The limitation is met by the transferring of patient between external sources (see: column 3, lines 36-42). The Examiner considers the transferring of the patient record (sync file) to be creating a patient folder one the information is received at a remote location.

10. Claims 25-26 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,924,074 to Evans.

As per claims 25-26, Evans teaches the transfer of patient data from the electronic medical records system to other healthcare providers as well as the updating of patient's record upon a nurses or physician entry of information into the system (see: column 4, lines 64 to column 5, lines 8, column 3, lines 36-42 and column 5, lines 29-40). In addition, Evans further teaches a tiered password system to ensure patient confidentiality and provides several levels of security for access to patient data (see: column 15, lines 9-32).

Although Evans fails to teach the remote system operates in an unattended mode that allows the electronic medical data to be transferred without operator input. Evans teaches that information is updated and transferred upon input by an authorized and the Examiner considers the feature of transferring data in an unattended mode to be merely automatically updating or transferring the data without an operator inputs and an old and well-known feature in the art. Therefore, it would have been obvious to a person of ordinary skill in the art to include

automatically updating or transferring data without an operator inputs within the system as taught by Evans with the motivation of providing an up-to-date medical record to authorized personnel to better treat the patient.

As per claim 32, it is rejected for the same reasons set forth in claims 25-26.

11. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,924,074 to Evans and U.S. Patent No. 6,305,377 to Portwood et al. in view U.S. Patent No. 6,370,841 to Chudy et al.

As per claim 34, Evans and Portwood et al. teach a record server and record client coupled to the record server (see: Evans: column 14, lines 8-16).

Evans and Portwood et al. fails to teach a data reader that reads the verification data from the package.

Chudy et al. teaches automated method for dispensing bulk medication that uses scanner device (129) for transmitting scanned code to the computer (119, Fig. 25) and generating a signal for computer (119, Fig. 25) to confirm that the package correspond to the patient's drug prescription information (see: column 14, lines 54-63).

One of ordinary skill in the art at the time the invention was made would have found it obvious to include the scanner device for reading and transmitting prescription information as taught by Chudy et al. within the electronic medical record system as taught by Evans with the motivation of storing a broad range of prescription information and the ability to fill patient prescription in rapid and efficient manner (see: column 1, lines 31-33).

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claims 24 and 27 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,924,074 to Evans.

As per claim 24, Evans teaches an electronic medical record system where upon the creation of a patient record, the patient locator (200, Fig. 13) creates a patient data structure (210, Fig. 13) having the PID and the patient's name (see: column 8, lines 29-31). The patient data structure (210, Fig. 13) maintains a pointer to an interface files structure (211, Fig. 13) having patient data transmitted from external sources (see: column 8, lines 36-38). In addition, the patient data structure (210, Fig. 13) may maintain a pointer to a legacy files structure (219, Fig. 13) having patient data transmitted from the legacy data system (106, Fig. 1), such as an image of a patient chart (see: column 8, lines 57-60).

As per claim 27, Evans teaches an electronic medical record system that transfers patient data from the electronic medical records system to other healthcare providers and between external sources (see: column 3, lines 36-42 and column 4, lines 64 to column 5, lines 8). In addition, Evans teaches the use of progress notes (144, Fig. 4) to summarize details of the patient's condition and to review the patient's progress over time (see: column 6, lines 31-36). The Examiner considers the progress notes (144, Fig. 4) to be transferred from healthcare providers to another.

Response to Arguments

Applicant's arguments with respect to claims 1-35 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert W. Morgan whose telephone number is (571) 272-6773. The examiner can normally be reached on 8:30 a.m. - 5:00 p.m. Mon - Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on (571) 272-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Robert Morgan
Patent Examiner
Art Unit 3626